UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA
PITTSBURGH DIVISION

LARA WILLIAMS, *individually and on behalf of all others similarly situated,* *Plaintiff*, v. **ECKERT SEAMANS CHERIN & MELLOTT, LLC**, *Defendant*.	INDEX NO.: **CLASS ACTION COMPLAINT** **JURY DEMAND**

PLAINTIFF'S CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Lara Williams ("Mrs. Williams" or "Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint ("Complaint") against Defendant, Eckert Seamans Cherin & Mellott, ("Eckert Seamans" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

I. INTRODUCTION

1. This class action arises out of Defendant's recent data security incident that occurred on or around the date(s) of April 17, 2025, in which cybercriminals exploited known vulnerabilities in the Defendant's computer network systems ("CNS") to gain access to and steal data Defendant obtained, collected, and maintained; causing Defendant to disclose the personally identifiable information ("PII" or "Private Information") of the Plaintiff and Class Members (defined below) to unauthorized third parties.

2. Mrs. Williams and Class Members, upon information and belief, are each and all alumni of Wheeling Jesuit University.

3. Defendant Eckert Seamans is a Pennsylvania domestic restricted professional limited liability company [1]that offers legal services and representation for entities and individuals.[2]

4. As a full-service national law firm with approximately 275 lawyers across a network of 15 offices, Eckert Seamans provides its clients with proactive, solution-oriented business and litigation counsel.[3]

5. Wheeling University is a private accredited higher learning institution located in Wheeling, West Virginia.[4] The alumni of Wheeling University count for more than 11,000 today.[5]

6. In the ordinary course of becoming a part of the Wheeling University Alumni group current and/or former Wheeling University students ("the putative class members") are encouraged and/or are obligated to provide Wheeling University with their Private Information to obtain enrollment in the school and gain access to the Wheeler Jesuit Alumni benefits and community.

7. The Private Information included but is not limited to the Plaintiff's and Class Member's "name and social security number" *See* Notice of Data Breach, attached hereto as Exhibit A.

8. In the ordinary course of business and as part of a former legal representation Eckert Seamans obtained, collected, and maintained, and Wheeling University did provide to Eckert Seamans, the private identifying information from but, upon information and belief not limited to,

[1] Pennsylvania Department of State --available at: https://file.dos.pa.gov/search/business (last visited June 30, 2025)
[2]Eckert Seamans, Our Firm – available at: https://www.eckertseamans.com/our-firm/about-our-firm (last visited June 30, 2025).
[3] *Id*.
[4] Wheeling University – available at: https://wheeling.edu/ (last visited June 30, 2025).
[5] Wheeling University, About, History – available at: https://wheeling.edu/about/history/ (last visited June 30, 2025).

Wheeling University Alumni as of 2019.[6] Defendant obtained, collected and maintained the Plaintiff's and Class Members' Private Information on its computer network systems ("CNS") centralized, upon information and belief, at its principal place of business.

9. Wheeling University entrusted Defendant with the Private Information on behalf of Plaintiff and Class members with the understanding that Defendant would reasonably protect the Private Information on behalf of Plaintiff and Class Members.

10. Upon information and belief, Defendant was on notice that failure to implement adequate and reasonable cyber-security procedures and protocols left the information held on Defendant's computer network systems in a dangerous condition and knew the risk of a data security incident occurring and leading to the improper disclosure of Plaintiff's and Class Members' Private Information.

11. Defendant's computer network systems lacked the adequate and reasonable cyber-security procedures and protocols, creating exploitable vulnerabilities in the CNS, leaving the Plaintiff's and Class Members' Private Information unprotected from the risk of improper disclosure.

12. Upon information and belief, cyber-criminals exploited the vulnerabilities in Defendant's computer network systems and accessed, encrypted, and stole the Private Information held by Defendant, which included the Plaintiff and Class Members' Private Information.

13. The Private Information remains in the hands of the cyber-criminals to this day and is likely to be disclosed on the dark web or to data brokers.[7]

14. Plaintiff brings this class action lawsuit, on behalf of those similarly situated, to address Defendant's inadequate safeguarding of Class Members' Private Information and for

[6] *See* Notice of Data Security Incident, Exhibit A
[7]

failing to provide adequate notice of the Data Breach to Plaintiff and other Class Members.

15. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed, disclosed, encrypted and/or taken as a result of Defendants negligent conduct.

16. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

17. Accordingly, Plaintiff sues Defendant seeking redress for their unlawful conduct and asserts claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract, and (iii) unjust enrichment.

II. PARTIES

18. Plaintiff Lara Williams at all times mentioned herein is an individual citizen of Ohio, residing in the city of Dillonvale.

19. Defendant Eckert Seamans, is a Pennsylvania-based domestic restricted professional limited liability company with its headquarters and principal place of business at 600 Grant St. 44th Fl, Pittsburgh, PA 15219.[8]

20. Defendant can be served through its registered agent, Scott Cessar, at 600 Grant St. 44th Fl, Pittsburgh, PA 15219.[9]

III. JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action under the Class Action

[8] Pennsylvania Department of State --available at: https://file.dos.pa.gov/search/business (last visited June 30, 2025).
[9] Secretary of the Commonwealth of Massachusetts – available at: https://corp.sec.state.ma.us/CorpWeb/CorpSearch/CorpSummary.aspx?sysvalue=9ylwf1SCbPtNUbHmo36065ww.h93oanSS0t9z_kUoHQ- (last visited June 30, 2025).

Fairness Act ("CAFA") 28 U.S.C. § 1332(d) because the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs and a member of the class is a citizen of a State different from the defendant.

22. This court has personal jurisdiction over Defendant because Defendant conducts business in this District, maintains its principal place of business in this District, and has sufficient minimum contacts with this State.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant's principal place of business is in this District and therefore resides in this District and a substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

IV. FACTUAL ALLEGATIONS

A. *DEFENDANT'S BUSINESS*

24. Defendant Eckert Seamans is a full-service national law firm with approximately 275 lawyers across a network of 15 offices, providing clients with proactive, solution-oriented business and litigation counsel.[10]

25. One of the areas that Eckert Seamans advertises to be expert in is Cybersecurity, Data Protection & Privacy.[11] Part of that expertise is providing counselling across industries regarding the protection of personal and other sensitive information.[12]

26. At a time currently unknown to the Plaintiff, Defendant represented Wheeling University in a legal matter, the subject which is unknown to Plaintiff, requiring Wheeling University to entrust Defendant with, but not limited to, the Private Information belonging to

[10] Eckert Seamans, Our Firm – available at: https://www.eckertseamans.com/our-firm/about-our-firm (last visited June 30, 2025).
[11] Eckert Seamans, Cybersecurity, Data Protection & Privacy – available at: https://www.eckertseamans.com/our-practices/data-privacy-security (last visited June 30, 2025
[12] *Id*.

Plaintiff and Class Members.

27. Plaintiff and Class Members are alumni of Wheeling University formerly represented by Defendant.

28. In the ordinary course of business, Defendant's clients and entities under Defendant's representation are encouraged and/or are mandated to provide (and Wheeling University on behalf of Plaintiff did provide) the Defendant with sensitive, personal, and private information, such as:

a. names and

b. Social Security numbers.[13]

29. On information and belief, Defendant stored this Private Information on its computer network system located at its principal place of business in Pennsylvania.

30. Based on the relationship between the Defendant and its current and former clients, including but not limited to alumni of Wheeling University, Defendant agreed to and undertook certain legal duties to maintain the confidentiality of the Private Information entrusted to it and to ensure that the Defendant's computer network system, containing the Private Information, is in compliance with all applicable laws, regulations and industry standards.

B. THE DEFENDANT HAD NOTICE OF THE RISK OF DATA BREACH AND IDENTITY THEFT

i) DEFENDANT HAS EXPERIENCE REPRESENTING ENTITIES IN DATA BREACH LITIGATION

31. Defendant knew the risk of data breaches posed by computer network systems without the proper protections.

32. Eckert Seamans has represented Cottonwood School District #242 in legal matters

[13] *See* Notice of Security Breach (Exhibit A).

concerning data breaches as recently as March 11, 2025.[14] Eckert Seamans has represented Penn LLC d/b/a PulseTV in legal matter concerning data breaches in March of 2022.[15]

ii) DEFENDANT HAS EXPERIENCE PROVIDING CYBERSECURITY GUIDANCE TO COMPANIES

33. In 2023, Matthew Meade, Chair of the Cybersecurity, Data Protection and Privacy Group at Eckert Seamans, moderated a panel discussing cybersecurity and data breach notifications at the Sedona Conference.[16]

34. On Defendant's blog, there are updates to state data breach laws provided to readers of the blog to keep them up to date on changes in the data breach legal landscape.[17] This Blog has also offered guidance on how to counsel clients in data breach response.[18].

35. Defendant has also prepared and delivered presentations about cybersecurity. Attorney Garfinkel for Defendant has presented and prepared guidance for Data Security: Risks, Compliance, and How to be Prepared for a Breach.[19]

36. Based on the Defendant's involvement in counseling, guiding and recommending actions to be taken by other entities in the name of Data Security, it follows that Defendant was on notice about the duty to safeguard private information and the potential injury that arises when those safeguards fail.

---

[14] Re: Notice of Data Security Incident, Office of the Idaho Attorney General (Mar. 11, 2025) – available at: https://www.ag.idaho.gov/content/uploads/2025/03/Cottonwood120264775.pdf (last visited June 30, 2025).
[15] Re: Supplemental Notic of Data Security Incident, Office of North Dakot Attorney General (Mar. 15, 2022) – available at: https://attorneygeneral.nd.gov/wp-content/uploads/2022/12/2022-03-22-PulseTV.pdf (last visited June 30, 2025).
[16] The Sedona Conference,Webinar on The Sedona Conference Commentary on Proposed Model Data Breach Notification Law – available at: https://thesedonaconference.org/webinar_TSC_Commentary_on_Proposed_Model_Data_Breach_Notification_Law
[17] Eckert Seamas, Legal Updates, Pennsylvania Updates State Data Breach Notification Law (Jul. 8, 2024) – available at: https://www.eckertseamans.com/legal-updates/pennsylvania-updates-state-data-breach-notification-law (last visited June 30, 2025).
[18] Eckert Seamans, Data Breach Response: How to Counsel Your Client (May 2015) – available at: https://www.eckertseamans.com/publications/data-breach-response-how-to-counsel-your-client
[19] https://www.eckertseamans.com/app/uploads/SandyGarfinkelpresentation091015.pdf

C. THE DATA BREACH

37. Defendant negligently maintained its computer network system in a condition that failed to meet the industry standards recommended by the ABA, the FTC, industry guides, and information technology security recommendations and manufacturers.

128. On June 18, 2025, Eckert Seamans confirmed it notified 9,400 people of an April 17, 2025 data breach that compromised names and Social Security numbers.[20]

129. A Data Breach occurs when unauthorized cyber criminals access a computer network system that has not been adequately and reasonably secured.

130. On or about June 18, 2025, Defendant mailed Plaintiff a "Notice of Data Security Incident"[21] that stated in part:

> What Happened:
>
> On April 17, 2025, we became aware of suspicious activity occurring on an attorney's computer. We immediately began an investigation with the assistance of a nationally recognized digital forensics firm and notified law enforcement. Our IT team quickly contained this incident. Through our investigation, we learned that an unauthorized actor accessed the attorney's computer and a limited amount of firm data that the attorney had access to on Ecker Seaman's network and then copied some of those files, including a 2019 document identifying Wheeling Jesuit alumni. Once we learned this, we conducted a thorough review of the impacted files to determine: (1) what information was involved; and (2) who may have been affected. On May 20, 20225, we competed the review and began working to locate address information to provide written notice to affected individuals.
>
> What Information was Involved:
>
> The information maintained on the list of Wheeling Jesuit alumni included your name and Social Security number

131. Plaintiff's notice letters were dated nearly one month after Defendant discovered

[20]

[21] Exhibit A

the Data Breach and nearly two months from the actual breach.

132. Within this notice, Defendant failed to state whether it was able to contain or end the cybersecurity threat, leaving victims in fear of their Private Information being leaked to the public or offered for sale to the public by data brokers and whether their Private Information that Eckert Seamans continues to maintain is secure.

133. Defendant also failed to state how the breach itself occurred.

134. All this information is vital to victims of a data breach due to the sensitivity, importance and value of the Private Information compromised in this specific breach.

135. Plaintiff and Class Members through Wheeling University provided Defendant with their Private Information reasonably expectating and believing that Defendant had implied a promise and accepted the responsibility to keep such information confidential and secure from unauthorized access as part of their contract to do business together.

136. Defendant's data security obligations were particularly important given the substantial increase in Data Breaches in the legal representation industry preceding the date of the breach.

137. In 2023, a record 3,205 data breaches occurred, resulting in around 353,027,892 individuals' information being compromised, a 78% increase from 2022.[22] In 2024, the ABA Cyber Security Report stated that 25% of law firms have previously suffered a data breach.

138. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

139. Therefore, the increase in such attacks, and attendant risk of future attacks, was

[22] *See* Identity Theft Resource Center, *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited July 1, 2025)

widely known to the public and to anyone in Defendant's industry, including Defendant.

G. ***DATA BREACHES ARE PREVENTABLE***

140. Defendant failed to use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

141. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

142. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[23]

143. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

23 How to Protect Your Networks from RANSOMWARE, at 3, available at: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited July 1, 2025)

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[24]

144. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

[24] *Id.* at 3-4.

Secure Internet-Facing Assets
- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene
- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege
- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure
- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[25]

145. Given that Defendant was storing the Private Information of its Client, Wheeling Jesuit University's alumni list Defendant could and should have implemented all the above measures to prevent and detect cyberattacks.

146. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of, upon information and belief,

[25] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last viewed July 1, 2025).

thousands to tens of thousands of individuals, including that of Plaintiff and Class Members.

i) Defendant Acquires, Collects & Stores Private Information

147. Defendant acquires, collects, and stores a massive amount of Private Information on its current and former clients.

148. By obtaining, collecting, and using Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

149. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

150. Upon information and belief, while collecting Private Information from Wheeling University, including Plaintiff, Defendant promised to provide confidentiality and adequate security for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

151. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

H. Defendant Fails to Comply with FTC Guidelines

152. The Federal Trade Commission ("FTC") has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

153. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines

note that businesses should protect the personal Private Information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[26]

154. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor incoming traffic for activity suggesting someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[27]

155. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

156. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect the Private Information in their possession by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an *unfair act or practice* prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.[emphasis added].

157. Defendant failed to properly implement basic data security practices.

158. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of

[26] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), *available at* www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 1, 2025).
[27] *Id*.

the FTC Act, 15 U.S.C. § 45.

159. Defendant was always fully aware of its obligation to protect the PII of its alumni of Wheeling University formerly represented by Defendant. Defendant was also aware of the significant repercussions that would result from its failure to do so.

I. DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

160. Confidentiality is a core tent of the legal profession.

161. At the ABA Annual Meeting in 2014, the ABA adopted a resolution on cybersecurity that encouraged all private and public sector organizations to develop, implement and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligation and is tailored to the nature and scope of the organization and the data and systems to be protected.

162. In fact, Rule 1.6: Confidentiality of Information of the American Bar Association (ABA), which states that lawyers should make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

163. Hackers target law firms due to the valuable information they hold, such as trade secrets, intellectual property, personally identifiable (PII), and confidential attorney-client privileged data.

164. Law firms have a duty to safeguard client information.

165. To comply with ABA obligations, it's vital to implement cybersecurity measures such as a plan, secure mobile devices, and vet legal tech providers.

166. The ABA recommends that law firms to do the following:

Conduct a risk assessment:

- Conduct regular risk assessments to identity if your firm has any key

vulnerabilities/weaknesses that could risk your clients' data privacy.
- Consider hiring a third party to conduct an independent audit, helping you identify cyber security gaps, create an Incident Response Plan, implement security measures, and train your staff on the latest best practices.
- It's also worth obtaining security certifications to understand your firm's risk and prove your security credentials. For example, ISO 27001 certification teaches firms everything they need to know, while also demonstrating their data security prowess to potential clients.

Develop a robust law firm cyber security policy and incident response plan:
- Each policy must be designed around the firm's unique, specific needs.
- Thoroughly audit their potential risk areas.
- create a customized policy taking these weaknesses into account, and
- ensure everyone on their staff is aware of their cyber security duties.

Use cyber security tools:
- Use comprehensive, up-to-date tools to safeguard their data security. i.e., spam filters, software-based filters, hardware-based filters.
- Implement robust data security encryption and protection, such as using multi-factor authentication and encrypting data in storage.[28]

167. To mitigate the risks of data breaches, legal professionals must stay updated on the latest technology trends.

168. Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including, without limitation, PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

169. These foregoing frameworks are existing and applicable industry standards in the legal industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

[28] *Cyber Security for Law Firms: What Lawyers Need to Know*, Clio, Braithwaite, C. (May 21, 2024) – available at: https://www.clio.com/blog/cyber-security-law-firms/ (last visited June 30, 2025).

IX. DEFENDANT'S BREACH

170. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect alumni of Wheeling University Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

e. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

171. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

172. Plaintiff and Class Members now face an increased risk of fraud and identity theft.

A. PLAINTIFF AND THE CLASS MEMBERS HAVE AND WILL EXPERIENCE SUBSTANTIAL HARM

173. Plaintiff and members of the proposed Class have suffered injury from the access, disclosure and misuse of their PII that can be directly traced to Defendant.

174. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII

secure are severe. Identity theft occurs when someone uses another's personal information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

175. Because of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- The loss of the opportunity to control how their PII is used;
- The diminution in value of their PII;
- The compromise and continuing publication of their PII;
- Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- Delay in receipt of tax refund monies; Unauthorized use of stolen PII; and
- The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

i) VALUE OF PRIVATE INFORMATION

176. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals often post stolen private information openly and directly on various "dark web" internet websites, making the

information publicly available, for a substantial fee of course.

177. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[29] For example, Personal Information can be sold at a price ranging from $40 to $200.[30] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[31]

178. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

179. One such example of criminals using PII for profit is the development of "Fullz" packages.

180. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

181. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and

---

[29] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last viewed July 1, 2025)

[30] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last viewed July 1, 2025)

[31] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last viewed July 1, 2025)

sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is traceable to the Data Breach.

182. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims, and the numbers are only rising.

183. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good" Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen.

184. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

185. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

186. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class

will need to remain vigilant against unauthorized data use for years or even decades to come.

187. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[32]

188. The FTC has also issued many guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires:

- encrypting information stored on computer networks;
- retaining payment card information only as long as necessary;
- properly disposing of personal information that is no longer needed;
- limiting administrative access to business systems;
- using industry-tested and accepted methods for securing data;
- monitoring activity on networks to uncover unapproved activity;
- verifying that privacy and security features function properly;
- testing for common vulnerabilities; and
- updating and patching third-party software.

189. According to the FTC, unauthorized PII disclosures ravage consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[33]

[32] Statement of FTC Commissioner Pamela Jones Harbour-Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009).(last visited July 1, 2025)

[33] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited July 1, 2025).

190. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

191. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

192. Plaintiff and Class Members now face an increased risk of fraud and identity theft.

B. DATA BREACHES PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTITY THEFT

193. Data Breaches such as the one experienced by alumni of Wheeling University which was formerly represented by Defendant are especially problematic because of the disruption they cause to the daily lives of victims affected by the attack.

194. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[34]The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[35]

195. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face

[34] 17 C.F.R. § 248.201 (2013).
[35] *Id.*

"substantial costs and time to repair the damage to their good name and credit record."[36]

196. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (possibly an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[37]

197. Identity thieves use stolen personal information such as Social Security numbers for various crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

198. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

199. Theft of Private Information is gravely serious. PII is a valuable property right.[38] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward

---

[36] U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (last visited July 1, 2025) ("GAO Report").

[37] Federal Trade Commission, *What To Do Right Away* (2024), *available at* https://www.identitytheft.gov/Steps (last visited July 1, 2025).

[38] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

analysis illustrates beyond doubt that Private Information has considerable market value.

200. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which studied data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

201. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

202. There is a strong probability that all the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

203. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[39]

204. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

[39] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), *available at* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited July 1, 2025).

205. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for more credit lines.[40]

206. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[41]

207. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

208. It is also hard to change or cancel a stolen Social Security number.

209. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[42]

210. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

X. PLAINTIFF'S EXPERIENCE

211. Plaintiff Lara Williams is and at all times mentioned herein was an individual

---

[40] Social Security Administration, *Identity Theft and Your Social Security Number* (2018), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 1, 2025).
[41] *Id* at 4.
[42] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (February 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited July 1, 2025).

citizen of Ohio, residing in the city of Dillonvale.

212. Plaintiff provided Defendant with her sensitive PII to obtain enrollment in Wheeler Jesuit University and obtain access to the Wheeler Jesuit Alumni benefits and community. Plaintiff received notice of the Data Breach around June 18, 2025, informing her that her sensitive information was part of Defendant's Data Breach (Exhibit A).

213. Plaintiff is careful about sharing her sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

214. Plaintiff stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her sensitive online accounts.

215. Had Plaintiff been aware that Defendant's computer systems were not secure, she would not have entrusted her personal data to Defendant.

216. Because of the Data Breach, Defendant advised Plaintiff to take certain steps to protect her Private Information and otherwise mitigate her damages.

217. Because of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. This time was spent at Defendant's direction by way of the Data Breach notice where Defendant recommended that Plaintiff mitigate her damages by, among other things, monitoring her accounts for fraudulent activity.

218. Even with the best response, the harm caused to Plaintiff cannot be undone.

219. Plaintiff suffered actual injury in the form of damages to and diminution in the

value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and have anxiety and increased concerns for the loss of her privacy.

220. Plaintiff has suffered imminent and impending injury arising from the exacerbated risk of fraud, identity theft, and misuse resulting from their Private Information being placed in the hands of criminals.

221. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches

XI. PLAINTIFF AND CLASS MEMBERS DAMAGES

222. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered inadequate identity monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

223. The credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. What's more, Defendant places the burden on Plaintiff and Class Members by requiring them to expend time signing up for that service rather than automatically enrolling all victims of this Data Breach.

224. Defendant's credit monitoring advice to Plaintiff and Class Members places the

burden on Plaintiff and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach.

225. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

226. Plaintiff's Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

227. Plaintiff and Class Members were damaged in that their Private Information is in the hands of cyber criminals.

228. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

229. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

230. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

231. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

232. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs

directly or indirectly related to the Data Breach.

233. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Many courts have recognized the propriety of loss of value damages in related cases.

234. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

235. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing “freezes” and “alerts” with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed because of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

236. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password protected.

237. Further, because of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

238. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

XII. CLASS REPRESENTATION ALLEGATIONS

239. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

240. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

241. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons in the United States who were notified their Private Information was compromised because of the April 17, 2025 Data Breach (the "Class").**

242. Excluded from the Class are Defendant's officers and directors, and any entity in

which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

243. Plaintiff reserves the right to amend or modify the class definitions with greater specificity or division after having an opportunity to conduct discovery.

244. This action satisfies the numerosity, commonality, typicality, and adequacy of requirements under Federal Rules of Civil Procedure 23.

245. Numerosity. In accordance with Fed. R. Civ. P. 23(a)(1), the Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiff now, but Defendant has provided notice to the Office of the Maine Attorney General that the number includes at least 9,400 individuals.[43]

246. Commonality. In satisfaction of Fed. R. Civ. P. 23(a)(2), there are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach adhered to industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard

[43] *See* OFFICE OF THE MAINE ATTORNEY GENERAL

their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Plaintiff and Class Members suffered legally cognizable damages from Defendant's misconduct;

i. Whether Defendant's conduct was negligent;

j. Whether Defendant's conduct was *per se* negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant was unjustly enriched;

m. Whether Defendant failed to provide notice of the Data Breach promptly; and

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

247. Typicality. Pursuant to Fed. R. Civ. P. 23(a)(3) Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, among other things, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and no defenses are unique to Plaintiff. Plaintiff's claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

248. Adequacy of Representation. As Fed. R. Civ. P. 23(a)(4) requires Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation

of this kind.

249. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

250. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy.

251. This class action is maintainable under Fed. R. Civ. P. 23 because the prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

252. This class action is maintainable under Fed. R. Civ. P. 23 because Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

253. Likewise, issues that will arise in this case are appropriate for certification under FRCP 23 because such issues are common to the Class, the resolution of which would advance

matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable considering best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

254. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

XIII. CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

255. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

256. Defendant required its corporate clients to provide on behalf of Plaintiff and Class Members non-public personal information as a condition of providing legal representation.

257. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure

and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

258. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

259. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and its corporate clients, which is recognized by laws and regulations as well as common law. Defendant could ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

260. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

261. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

262. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

263. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

264. Failing to adequately monitor the security of its networks and systems;

265. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

266. Allowing unauthorized access to Class Members' Private Information;

267. Failing to detect timely that Class Members' Private Information had been compromised;

268. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

269. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

270. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the legal industry.

271. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

272. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

273. Defendant's negligent conduct is ongoing, in that they still hold the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

274. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

SECOND COUNT
NEGLIGENCE PER SE
(On Behalf of Plaintiff and All Class Members)

275. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

276. Under the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

277. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

278. Defendant breached its duties to Plaintiff and Class Members under Pennsylvania law by failing to develop and implement policies and procedures necessary to protect Plaintiff's and Class Members' PII.

279. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

280. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

281. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that by failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

282. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

THIRD COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

283. Plaintiff re-alleges and incorporate the above allegations as if fully set forth herein.

284. When Plaintiff and Class Members provided their Private Information to Wheeling University who in turn provided it to Defendant in exchange for legal representation they entered implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

285. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

286. In entering such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant federal and state laws and regulations, and adhered to industry standards.

287. Plaintiff and Class Members paid money to Defendant or provided labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

288. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

289. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to

ensure that they adopted reasonable data security measures.

290. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

291. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

292. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged here, including the loss of the benefit of the bargain.

293. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

294. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FIFTH COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

295. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

296. Plaintiff brings this claim individually and on behalf of all Class Members. This count is pled in the alternative to the breach of implied contract count above.

297. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

298. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the portion of each payment made that is allocated to data security is known to Defendant.

299. Plaintiff and Class Members conferred a monetary benefit on Defendant. Defendant's acceptance and storage of Plaintiff's and the other Class members' Private Information created a fiduciary relationship between Defendant on the one hand, and Plaintiff and the other Class members, on the other hand. In light of this relationship, Defendant must act primarily for the benefit of its corporate clients' employees, clients, and/or customers, which includes safeguarding and protecting Plaintiff's and the other Class members' Private Information.

300. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

301. Defendant enriched itself by saving the costs Defendant reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Rather than providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by using cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

302. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

303. Defendant failed to secure Plaintiff's and Class Members' Private Information and thus did not provide full compensation for the benefit Plaintiff and Class Members provided.

304. Defendant acquired the Private Information through inequitable means in that they

failed to disclose the inadequate security practices alleged.

305. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

306. Plaintiff and Class Members have no adequate remedy at law.

307. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the loss of the opportunity of how their Private Information is used;

c. the compromise, publication, and/or theft of their Private Information;

d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information;

e. lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;

f. the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and

g. future costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the effect of the Private Information compromised because of the Data Breach for the rest of the lives of Plaintiff and Class Members.

308. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

309. Defendant should be compelled to disgorge into a common fund or constructive

trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

XIV. PRAYER FOR RELIEF

310. WHEREFORE, Plaintiff, on behalf of herself and the Class described above seek the following relief:

a. For an Order certifying this action as a class action, defining the Class as requested herein, appointing Plaintiff and their counsel to represent the Class, and finding that Plaintiff are proper representatives of the Class requested herein;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained because of Defendant's wrongful conduct;

e. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and

j. Any other relief that this court may deem just and proper.

XV. JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: July 8, 2025

/s/ Jacob Ginsburg
Jacob U. Ginsburg, Esq. (311908)
Kimmel & Silverman PC
30 E. Butler Ave.
Ambler, PA 19002
(267) 468-5374
jginsburg@creditlaw.com

Leigh S. Montgomery*
Texas Bar No. 24052214
lmontgomery@eksm.com
EKSM, LLP
4200 Montrose Blvd. Ste 200
Houston, Texas 77006
Phone: (888) 350-3931

ATTORNEYS FOR PLAINTIFF AND THE PUTATIVE CLASS
(* denotes *pro hac vice* forthcoming)